修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　情報システム学研究科　情報ネットワークシステム学専攻　博士前期課程		
氏　　名	入口　吉信	学籍番号	0852005
論 文 題 目	多数回の配信でブラックリストによって結託犯を追跡する結託耐性符号化及び運用法		

要　　旨

動画像コンテンツの配信サービスやオンライン販売などにおいて，利用者による不正コピーを防止する技術が必要不可欠である．電子指紋では利用者を特定するための情報（指紋）をコンテンツの配布時に電子透かしとして埋め込んでおき，利用者がコンテンツを不正にコピーし，サービス提供者が不正コピーを見つけた場合，透かしからばらまいた者を特定する．電子指紋を利用する場合，複数人が各自のコピーを比較することで電子透かしの埋め込まれた場所を特定し改変・無効化する結託攻撃がおこりうる．

結託耐性符号は，符号語を指紋としたときに結託攻撃を受けても結託犯（colluder）の追跡ができるように構成された符号である．本研究では簡易な結託耐性符号である Boneh-Shaw 符号と，それを連接し符号長を改善した c-secure CRT 符号を扱う．結託攻撃には特に重要なものとして無作為，多数決，少数決，最大値，最小値の五つがある．

一方，不正利用者の処遇として，のちに利用禁止措置をとることにはなろうが，いったんブラックリストに登録することがあげられる．

本研究は複数回のコンテンツ配信をおこなう場合に，結託集団のメンバが固定されていることを条件にブラックリストを用いることでより結託犯の追跡が効率よくできることを示す．ブラックリストには追跡された結託犯が順次登録されるようにし，コンテンツ配布を繰り返すことでより早く結託集団全員を追跡可能である．また，結託集団に割り当てる符号語の差を，ホワイトリストによって大きくすることで，結託集団がブラックリストに載っているメンバを推測しにくくする方法を示す．c-secure CRT 符号では，符号の構成法を修正することでブラックリスト割り当て方式を適用でき，とくに無作為攻撃で追跡効率が上がることを示す．